Lecture 11.

Golay Codes

Recall that inner product of two vectors $v = (\alpha_1, \dots, \alpha_n)$ and $w = (\beta_1, \dots, \beta_n)$ is defined as

$$v \cdot w = \sum_{i=1}^{n} \alpha_i \beta_i .$$

In this section we consider only linear codes.

Def: A code $C \subset \cancel{Z} F^n$ is ~~sef~~ self-orthogonal if $C \subseteq C^\perp$, that is, $C \cdot C = (0)$.

Def: A code C is self-dual if $C^\perp = C$.

Let C be an $[n,k]$-code. Then $C^\perp$ is a $[n, n-k]$-code. If C is self-orthogonal then $k \le n-k$, $k \le \frac{n}{2}$. If C is self-dual then $k = \frac{n}{2}$. This is possible only if n is even.

In a linear self-orthogonal code C

if $v = (\alpha_1, \dots, \alpha_n) \in C$ then $\alpha_1^2 + \dots + \alpha_n^2 = 0$. If $F = \mathbb{Z}(2)$ then $wt(v)$ in this case is even.

Now let us consider binary codes, i.e. assume that $F = \mathbb{Z}(2)$.

<u>Def.</u> A code C is <u>even</u> if all vectors $v \in C$ have even weights.

A self-orthogonal code is even.

<u>Def.</u> A code C is <u>doubly-even</u> if all vectors $v \in C$ have weights that are multiples of 4.

<u>Lemma.</u> A binary linear code with a generator matrix G is self-orthogonal if and only if the rows of G are pairwise orthogonal and all rows have even weights.

<u>Proof.</u> Obvious.

For an n-tuple $a = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$ let $\bar{a}$ be the vector of remainders $\bar{a} = (\bar{\alpha}_1, \ldots, \bar{\alpha}_n)$, here $\bar{\alpha}_i$ is the remainder of α_i mod 2. Let $a' = (\alpha_1', \ldots, \alpha_n') \in \mathbb{Z}^n$, $\alpha_i' = 1$ if $\bar{\alpha}_i = 1$ and $\alpha_i' = 0$ if $\bar{\alpha}_i = 0$. Hence $a - a' \in 2 \cdot \mathbb{Z}^n$. We say that the vector $a' \in \mathbb{Z}^n$ <u>mimicks</u> the vector $\bar{a} \in \mathbb{Z}(2)^n$.

We notice that $wt\, \bar{a} = a' \cdot a'$.

<u>Lemma</u>. $a \cdot a = wt(\bar{a}) \mod 4$.

<u>Proof</u>. Let $a = a' + 2b$, $b \in \mathbb{Z}^n$. Then

$$a \cdot a = a' \cdot a' + 4\, a' \cdot b + 4\, b \cdot b$$

Now it is clear that $a \cdot a = a' \cdot a' \mod 4$, which completes the proof. ⊥

<u>Lemma.</u> A binary linear self-orthogonal code C with a generator matrix G is doubly-even if and only if all rows of G have weights divisible by 4.

<u>Proof.</u> Let $G = \begin{pmatrix} \bar{a}_1 \\ \vdots \\ \bar{a}_k \end{pmatrix}$, $\bar{a}_i$'s are rows of the matrix G. Let a_i be the 0,1-vector in $\mathbb{Z}^n$ that "mimicks" the vector $\bar{a}_i$.

All weights $wt(\bar{a}_i)$ are multiples of 4 and $\bar{a}_i \cdot \bar{a}_j = 0$.

Let $\bar{a} = \bar{a}_{i_1} + \dots + \bar{a}_{i_p}$. We need to show that the $wt(\bar{a})$ is a multiple of 4. Consider the vector $a = a_{i_1} + \dots + a_{i_p}$. Then $\bar{a}$ is the vector of remainders of components of a. By the

Lemma above $a \cdot a = wt(a) \bmod 4$. By the same Lemma all inner squares $a_{i_1} \cdot a_{i_1}, \dots$ $\dots, a_{i_p} \cdot a_{i_p}$ are multiples of 4. We have also $a_{i_\mu} \cdot a_{i_\nu} \in 2 \cdot \mathbb{Z}^n$, $1 \le \mu, \nu \le p$. Now,

$$a \cdot a = \cancel{\neq} a_{i_1} \cdot a_{i_1} + \dots + a_{i_p} \cdot a_{i_p} + 2 \sum_{\mu < \nu} a_{i_\mu} \cdot a_{i_\nu} = 0 \bmod 4$$

This completes the proof of the lemma.

Cyclic Matrices.

$$\begin{pmatrix} a_1 \cdots a_{n-1} \; a_n \\ a_n \; a_1 \cdots a_{n-1} \\ a_{n-1} \; a_n \; a_1 \cdots a_{n-2} \\ \cdots \end{pmatrix}$$

Let us consider an 11×11 cyclic matrix over $\mathbb{Z}(2)$

$$A = \left.\begin{pmatrix} 0\,1\,0\,0\,0\,1\,1\,1\,0\,1\,1 \\ 1\,0\,1\,0\,0\,0\,1\,1\,1\,0\,1 \\ 1\,1\,0\,1\,0\,0\,0\,1\,1\,1\,0 \\ 0\,1\,1\,0\,1\,0\,0\,0\,1\,1\,1 \\ \dots \\ \\ \end{pmatrix}\right\} 11$$

1) the inner product of any two different rows is $\neq 0$ in $\mathbb{Z}(2)$;

2) the weight of every row is 6;

3) $wt(\bar{a}_i + \bar{a}_j) = 6$, $i \neq j$. Hence

$$wt(\bar{a}_i + \bar{a}_j + \underbrace{(1\,1 \dots 1)}_{11}) = 5;$$

4) $wt(\bar{a}_i + \bar{a}_j + \bar{a}_k) = 3$; i, j, k distinct;

5) any 4 rows are linearly independent.

Consider a code C with the generation matrix

$$G = \left(\begin{array}{cccc|c|cccc} 1 & & & 0 & 1 & & & & \\ & 1 & & & \vdots & & A & & \\ & & \ddots & & 1 & & & & \\ 0 & & & & 1 & & & & \\ & & & 1 & 0 & 1 & 1 & \cdots & 1 \end{array}\right)$$

This is a 12×24 matrix. The weight of the last 12-th row is 12. The weights of the other rows are $= 6+1+1=8$.

Because of 1) and 2) all rows are pairwise orthogonal.

Hence, by the Lemma the code C is a doubly-even code. Since all weights of rows are even and rows are pairwise orthogonal it follows that the code C is self-orthogonal, $C \subseteq C^{\perp}$. Since the dimension of C is 12 the dimension of $C^{\perp}$ is also 12. Hence $C = C^{\perp}$, the code

C is self-dual.

Let us show that $d=8$. Since the code is doubly-even it follows that the minimal weight is 4 or 8.

Let us show that C does not contain vectors of weight 4.

Suppose that v is a sum of rows of the matrix G and $wt(v)=4$.

A sum of ≥ 5 rows of the matrix G has weight ≥ 5 even in the first 12 columns.

Let v be a sum of 4 rows. Since v has weight 4 in the first 12 columns, the projection of v to the last 12 columns is 0.

If the 12th row is involved then v has 1 in the column 13. If the 12-th row is not involved then the sum of 4 rows of the matrix A is $=0$, which contradicts 5).

Let v be a sum of 3 rows. Then the weight of v in the last 12 columns is $=1$. Suppose that the 12-th row is involved. Then $wt(\bar{a}_i + \bar{a}_j + (\underbrace{1\,1\,\cdots 1}_{11})) = 1$, which contradicts 3). Suppose now that the 12-th row is not involved. Then v has one in the column 13 and therefore $\bar{a}_i + \bar{a}_j + \bar{a}_k = 0$ for 3 distinct rows of the matrix A, which contradicts 4) and 5).

Let v be a sum of two rows, the weight in the last ~~two~~ 12 columns is $=2$. If the 12-th row is involved then v has 1 in the 13-th column and $wt(\bar{a}_i + \underbrace{(11\ldots1)}_{11}) = 1$, which contradicts 2).

If the 12-th row is not involved then $wt(\bar{a}_i + \bar{a}_j) = 2$, which contradicts 3).

If v is a row of the matrix G then $wt(v) = 8$ or 12.

We proved that the Hamming weight of the code C is 8.

The code C is called the <u>extended Golay code</u>. Notation: $G(24)$.

Now take any column of the matrix G and drop the j-th coordinate. In other words project $\mathbb{Z}(2)^{24} \to \mathbb{Z}(2)^{23}$.

The image of the code $G(24)$ is a code

with the minimal weight 7. The dimension will stay the same since ~~no column belongs to G(2~~ the vector $(0\cdots0\underset{j}{1}0\cdots0)$ does not belong to $G(24)$.

We have got the code $G(23)$ of the type $[23, 12, 7]$.

<u>Theorem.</u> The code $G(23)$ is perfect.

<u>Proof.</u> For $d=7$, $\left[\frac{d-1}{2}\right]=3$. The volume of $B(0,3)$ in $\mathbb{Z}(2)^{23}$ is: $1+23+\binom{23}{2}+\binom{23}{3}$

$$= 1+23+23\cdot 11+\frac{23\cdot 22\cdot 21}{6} = 24+253+\underbrace{23\cdot 11}_{253}\cdot 7 = 24+253\cdot 8 = 8\,(3+253)=8\cdot 256 =$$

$$= 2^3\cdot 2^8 = 2^{11};$$

$$|G(23)| = 2^{12} = \frac{2^{23}}{2^{11}}.$$

$\downarrow$

Theorem (V. Pless, we won't prove it). If C is a linear code in $\mathbb{Z}(2)^{24}$ of Hamming weight 8, then C is permutation equivalent to $G(24)$.

The ternary Golay code.

We will describe a ternary $[11,6,5]$ code of Golay. It is a perfect double error correcting code.

But first we will describe the extended ternary Golay code of the type $[12,6,6]$.

Let A be the cyclic 5×5 matrix

$$A = \begin{pmatrix} 0 & 1 & 2 & 2 & 1 \\ 1 & 0 & 1 & 2 & 2 \\ 2 & 1 & 0 & 1 & 2 \\ 2 & 2 & 1 & 0 & 1 \\ 1 & 2 & 2 & 1 & 0 \end{pmatrix}$$

1) For any two rows $\bar{a}_i, \bar{a}_j$, $i \neq j$,

$wt(\bar{a}_i + \bar{a}_j) = 3$, $wt(\bar{a}_i - \bar{a}_j) = 4$.

Let

$$G = \underbrace{\left(\begin{array}{ccc|c} 1 & & 0 & 1 \\ & 1 & & 1 \\ & & & 1 \\ & & & 1 \\ 0 & & \ddots & 1 \\ & & & 1 \\ & & 1 & 0 \end{array}\right.}_{6} \left.\begin{array}{c} \\ A \\ \\ \\ 1\,1\,1\,1\,1 \end{array}\right)\Bigg\} 6$$

The weight of every row of G is 6. The inner product of any two distinct rows of G is divisible by 3.

We repeat the old argument: let $a \in \mathbb{Z}^n$, $\bar{a}$ = the vector of remainders mod 3, a' is the vector from $\mathbb{Z}^n$ that mimicks $\bar{a}$.

So, $a = a' \mod 3 \cdot \mathbb{Z}^n$. Since $2^2 = 1 \mod 3$,

$wt\,\bar{a} = a' \cdot a' \mod 3 = a \cdot a \mod 3$.

Let $\bar{a} = \bar{a}_{i_1} \pm \dots \pm \bar{a}_{i_p}$ be a linear combination of rows. Let $a = a_{i_1} \pm \dots \pm a_{i_p}$. Then

$$a_i \cdot a_i = a_i' \cdot a_i' \bmod 3 = wt(\bar{a}_i) \bmod 3,$$

$$a \cdot a = \sum a_{i_\mu} \cdot a_{i_\mu} + 2 \sum_{\mu < \nu} a_{i_\mu} \cdot a_{i_\nu} = 0 \bmod 3.$$

It implies that $wt\, \bar{a}$ is divisible by 3.

Hence weight of a nonzero element from C is $= 3$ or 6.

Let us show that C does not contain a vector of weight 3. Let $v \in C$, $wt(v) = 3$. The vector v is a linear combination of rows of the matrix G.

If > 3 rows are involved then the weight in the first 6 coordinates is > 3.

If v is a row then $wt(v) = 6$.

Let v be a linear combination of two rows. The weight in the first 6 coordinates is 2. It is easy to see (Exercise!) that the weight of a linear combination of two rows of the 6×6 matrix $\begin{pmatrix} 1 & & \\ 1 & & A \\ \vdots & & \\ 1 & & \\ 0 & \underbrace{1\ 1 \cdots 1}_{5} & \end{pmatrix}$ is > 1.

If v is a linear combination of 3 rows then the weight in the first 6 columns is 3.

<u>Exercise.</u> Any 3 rows of $\begin{pmatrix} 1 & & \\ 1 & & A \\ \vdots & & \\ 1 & & \\ 0 & 1\ 1 \cdots 1 & \end{pmatrix}$ are linearly independent.

This proves that the Hamming weight of C is 6.

Again erasing one coordinate yields

a code of the type $[11, 6, 5]$.

The volume of the ball of radius 2 is:

$$1 + \binom{11}{1} \cdot 2 + \binom{11}{2} \cdot 2^2 = 1 + 22 + \frac{11 \cdot 10}{2} \cdot 4 =$$

$$= 1 + 22 + 22 \cdot 10 = 1 + 2 \cdot 11^2 = 1 + 2 \cdot 121 = 243$$

$$= 3^5.$$

Hence $3^6 = \frac{3^{11}}{3^5}$, the code is perfect.

<u>Theorem</u> (we won't prove it). A nontrivial linear perfect code is either a Hamming code or a Golay code.